技術情報:Si-R/Si-R brinシリーズ設定例

(「NET-G」とのVPN(IPsec)接続-IPv4_NATトラバーサルあり)

dit_NET-GとIPv4でVPN接続する場合の設定事例です。 NATトラバーサル機能を利用する場合の設定事例です。 NAT RouterではIPsecパススルー機能をoffにして下さい。

[対象機種と版数] Si-R Gシリーズ V4.06以降

[設定内容]

- ・Si-R Gのether 1 1をWAN側、ether 2 1-4をLAN側とします。
- ・NET-G側のルータでNAT機能を有効にします。
- ・LAN側に192.168.1.254/24、192.168.2.254/24を割り当てます。
- ・IKE/IPsecのパラメータを以下のように設定します。

ルに関連パニメータ		いっこの間 声 パニメーク	
		IPSEC国連ハリケータ	
キー交換モード	アグレッシブモード	プロトコル	ESP
暗号化アルゴリズム	AES-256	暗号化アルゴリズム	AES-256
整合性アルゴリズム	SHA2	整合性アルゴリズム	SHA2
DHグループ	1,536bit	DHグループ	1,536bit
事前共有鍵文字列	"sir2-key","sir3-key"	キーの有効時間	60分/100,000Kbyte
装置識別情報	"sir2","sir3"		
キーの有効時間	480分		



[設定例] ・sir2-keyにはIPsec鍵を設定してください。

Si-R G設定例

ether 1 1 vlan untag 1001 ether 2 1-4 vlan untag 1002 lan 0 ip address 10.10.1.1/24 3 lan 0 ip route 0 default 10.10.1.2 1 1 lan 0 vlan 1001 lan 1 ip address 192.168.1.1/24 3 lan 1 vlan 1002 template 0 name NET-G template 0 interface pool 1 50 template 0 aaa 0 template 0 datalink type ipsec template 0 ipsec ike protocol esp template 0 ipsec ike encrypt aes-cbc-256 template 0 ipsec ike auth hmac-sha256 template 0 ipsec ike pfs modp1536 template 0 ike mode aggressive template 0 ike proposal 0 encrypt aes-cbc-256 template 0 ike proposal 0 hash hmac-sha256 template 0 ike proposal 0 pfs modp1536 template 0 ike nat-traversal use on template 0 tunnel local 10.10.1.1 aaa 0 name sir aaa 0 user 0 id sir2 aaa 0 user 0 password sir2 aaa 0 user 0 ip route 0 20.1.1.1/32 1 1 aaa 0 user 0 ipsec ike range any4 20.1.1.1/32 aaa 0 user 0 ike shared key text sir2-key aaa 0 user 1 id sir3 aaa 0 user 1 password sir3 aaa 0 user 1 ip route 0 20.1.1.2/32 1 1 aaa 0 user 1 ipsec ike range any4 20.1.1.2/32 aaa 0 user 1 ike shared key text sir3-key syslog pri error, warn, info syslog facility 23 time zone 0900 consoleinfo autologout 8h telnetinfo autologout 5m terminal charset SJIS

解説 Si-R_G設定解説

Si-R G

ether 1 1 vlan untag 1001 ether 1 1ポートをTag なしVLAN1001に設定します。

ether 2 1-4 vlan untag 1002 ether 2 1-4ポートをTag なしVLAN 1002に設定します。

lan 0 ip address 10.10.1.1/24 3 LAN0側IPアドレスを設定します。 ・10.10.1.1/24 : IPアドレス/マスクです。 ・3 : ブロードキャストアドレスのタイプです。 通常は3で構いません。

lan 0 ip route 0 default 10.10.1.211
スタティックルートを設定します。
・default : デフォルトルートです。
・10.10.1.2 : ネクストホップです。
・1 : metric値です。通常はこのままで構いません。
・1 : distance値です。通常はこのままで構いません。

lan 0 vlan 1001 VLAN ID とlan 定義番号の関連付けを行います。

lan 1 ip address 192.168.1.1/24 3 LAN1側IPアドレスを設定します。 ・192.168.1.1/24 : IPアドレス/マスクです。 ・3 : ブロードキャストアドレスのタイプです。通常は3で構いません。

lan 1 vlan 1002 VLAN ID とlan 定義番号の関連付けを行います。

template 0 name NET-G インターフェースの名前(任意)を設定します

template 0 interface pool 1 50 テンプレート着信で使用するrmt インタフェースの設定をします。 ・1:テンプレート着信で使用する開始rmt インタフェース番号です。 ・50:テンプレート着信で使用するrmt インタフェース数です。。上記設定の場合、rmt1~rmt50の最大 50拠点分のtemplate着信が可能です。

template 0 aaa 0 テンプレート着信で認証および着信を行う場合に参照するAAA のグループIDを設定します。

template 0 datalink type ipsec パケット転送方法としてIPsecを設定します。

template 0 ipsec ike protocol esp 自動鍵交換用IPsec情報のセキュリティプロトコルにESP(暗号)を設定します。

template 0 ipsec ike encrypt aes-cbc-256 自動鍵交換用IPsec情報の暗号情報にAES256ビットを設定します。 template 0 ipsec ike auth hmac-sha256 自動鍵交換用IPsec情報の認証情報にSHA256を設定します。

template 0 ipsec ike pfs modp1536 自動鍵交換用IPsec情報のDH(Diffie-Hellman) グループにmodp1536を設定します。

template 0 ike mode aggressive IKE 情報の交換モードとしてAggressive Mode を設定します。

template 0 ike proposal 0 encrypt aes-cbc-256 IKEセッション用暗号情報の暗号アルゴリズムにAES256ビットを設定します。

template 0 ike proposal 0 hash hmac-sha256 IKE セッション用認証(ハッシュ) 情報にSHA256を設定します。

template 0 ike proposal 0 pfs modp1536 IKE セッション用DH(Diffie-Hellman) グループにmodp1536を設定します。

template 0 ike nat-traversal use on NATトラバーサル機能を有効にします。

template 0 tunnel local 10.10.1.1 IPsecトンネルの送信元アドレスの設定をします。

aaa 0 name sir AAA認証のグループ名を設定します。

aaa 0 user 0 id sir2 AAA認証に使用する、認証情報(ユーザID) を設定します。

aaa 0 user 0 password sir2 AAA認証に使用する、認証情報(認証パスワード)を設定します。 ・IPsecのAggressive Modeを利用する場合は、相手装置識別情報を設定します。 ・ユーザIDと認証パスワードは同じ値を設定してください。

aaa 0 user 0 ip route 0 20.1.1.1/32 1 1 スタティックルートを設定します。 ・20.1.1.1/32 : 宛先ネットワーク/マスクです。 ・1 : metric値です。通常は1で構いません。 ・1 : distance値です。通常は1で構いません。

aaa 0 user 0 ipsec ike range any4 20.1.1.1/32 自動鍵交換用IPsec 情報の対象範囲を設定します。 ・any4 : IPsec 対象となる送信元IP アドレス/マスクです。 ・20.1.1.1/32 : IPsec 対象となる宛先IP アドレス/マスクです。

aaa 0 user 0 ike shared key text sir2-key IKEセッション確立時の共有鍵(Pre-shared key)を設定します。 aaa 0 user 1 id sir3 AAA認証に使用する、認証情報(ユーザID)を設定します。

aaa 0 user 1 password sir3 AAA認証に使用する、認証情報(認証パスワード)を設定します。 ・IPsecのAggressive Modeを利用する場合は、相手装置識別情報を設定します。 ・ユーザIDと認証パスワードは同じ値を設定してください。

aaa 0 user 1 ip route 0 20.1.1.2/32 1 1 スタティックルートを設定します。 ・20.1.1.2/32 : 宛先ネットワーク/マスクです。 ・1 : metric値です。通常は1で構いません。 ・1 : distance値です。通常は1で構いません。

aaa 0 user 1 ipsec ike range any4 20.1.1.2/32 自動鍵交換用IPsec 情報の対象範囲を設定します。 ・any4 : IPsec 対象となる送信元IP アドレス/マスクです。 ・20.1.1.2/32 : IPsec 対象となる宛先IP アドレス/マスクです。

aaa 0 user 1 ike shared key text sir3-key IKEセッション確立時の共有鍵(Pre-shared key)を設定します。

syslog pri error,warn,info syslog facility 23 システムログ情報の出力情報/出力対象ファシリティの設定をします。通常はこのままで構いません。

time zone 0900 タイムゾーンを設定します。通常はこのままで構いません。

consoleinfo autologout 8h telnetinfo autologout 5m シリアルコンソール、TELNETコネクションの入出力がない場合のコネクション切断時間を設定します。通常はこの ままで構いません。

terminal charset SJIS ターミナルで使用する漢字コードをShift JISコードに設定します。 NET-G1の設定例になります。NET-G2についても同様に設定を行ってください。 「ポリシーエディタを実行」を選択します。

	■ 統計を表示(V)…	
	🚱 ポリシー エディタを実行(<u>E</u>)	
	監査(U)	•
	VPN を選択(<u>C</u>)	•
ъ	アクティブなポリシーの選択(<u>P</u>)	•
Clie	🚱 ポリシー マネージャを起動(S)	- 22
VPN	😗 ポリシー マネージャを停止(<u>T</u>)	
ure		
Sec	製品情報(P)	
1-G	 パージョン情報(<u>A</u>)…	
RE	トレイを隠す(<u>R</u>)	

鍵管理タブの「自分の鍵」を選択した状態で右クリックし、「追加」を選択します。

■ NET-G Secure VPN Client ポリシー エディタ 👔	23
セキュリティボリシー 鍵管理	
追加(D)… 削除(R) プロパティ(P)… 表示(V)…	
ローカル ホストの認証に使用される鍵です。	
OK キャンセル 適用	

新しい認証鍵		23
NET-G Secure VPN Client	このウィザードでは新しい認知証練を生成する手順を示します。	
12 Mars	作成する認証鍵の種類はどれですか?	
NOL A	◎ 認証鍵ペアと証明書を作成する(<u>C</u>)	
KAR	 · 新心,福祉引音,显显成,9,002 · · · · · · · · · · · · · · ·	
K TRA		
X4788		
	(<戻る(B) 次へ(N)> キャンション・ション・ション・ション・ション・ション・ション・ション・ション・ション	2411

共有シークレットの設定を行います。今回の設定例では共有シークレットはsir2-keyと設定しています。この設定 値はSi-R側のtemplate 0 ap 0 ike shared keyと一致している必要があります。名前はSi-R側の設定とは 関係がないので任意の名前を設定してください。

既知共有鍵(C自分だ 同入力にます。つく)	けが参照するための名i iiーブリントを使用して	前を付けます。入力ミスを防ぐ 実際にシークレットを表示せる	ために共有シークレットを 2 115通信相手とシークレットを	
面入りしょう。 フィンパ 確認します。	J-JJJFERMOC	大時間にノークレクトを強めたとう	「ここ題「書作日子」こと、アントントで	
名前:	Si-R2_shar	edkey		
共有シークレット				
共有シークレットの	·確認: ●●●●●●			J
フィンガープリント(SHA-1): 2c33 2ce5			

IDの設定を行います。ローカルIDおよびリモートIDを下のように設定してください。

ローカルのホストドメイン名"sir2"はSi-R側のtemplate 0 ap 0 ike name remoteと一致している必要があ ります。リモートのホストIPアドレス"10.10.1.1"はSi-R側のtemplate 0 ap 0 tunnel localと一致している 必要があります。設定が終了したら「完了」をクリックします。

۲	でのみ使用可能です。	2月19日にのの小小川山は4次に9。15 アドレス以外の 10 は、16ビアクレッシノモー
C	コーカル プライマリ ID:	■ ホスト ドメイン名 ・ ・ ・ ・ ・ ・ ・ ・
	ホスト ドメイン名:	sir2
IJ	ノモート プライマリ ID:	[1] ホスト ドメイン名
	ホスト ドメイン名:	10.10.1.1

「適用」をクリックします。

■ NET-G Secure VPN Client ポリシー エディタ セキュリティ ポリシー 鍵管理	88
 信頼されたポリシーサーバ 信頼された証明書 記証局 ゴート ホスト ディレクトリ サービス ティレクトリ サービス 自分の鍵 ディントキー as 証明書 追加 デ・R2_sharedkey 追加 	
道加(D) 肖耶翁(B) プロパティ(P) ま 説明 ローカル ホストの認証に使用される鍵です。	₩
OK キャンセル [適用

セキュリティーポリシータブの「VPN接続」を右クリックし、「規則を追加」を選択します。

	- 前フィルタ	
 	開<(<u>0</u>)	規
	規則を追加	則の
⊡- ा IPser	リストから選択	評
		価
		—————————————————————————————————————
追加(A)	前除(<u>R)</u> プロパラ	ティ(<u>P)</u>) [診断(<u>D</u>)
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		

ゲートウェイ名、リモートネットワーク、認証鍵の設定を行います。

ゲートウェイのIPアドレス"10.10.1.1"はSi-R側のtemplate 0 ap 0 tunnel localと一致している必要があります。リモートネットワーク"any"はSi-R側のtemplate 0 ap 0 ipsec ike rangeの送信元ネットワークと一致している必要があります(Si-Rの設定はany4となっており、ここで設定しているanyと同等です)。認証鍵の設定は先ほど共有シークレットで設定した任意の名前をプルダウンメニューから選択します。

PN 接続を追加	
→ ゲートウェイ名:	10.10.1.1 IP
 リモート ネットワーク: 	any 🔻 🛄
認証鍵:	🖙 Si-R2_sharedkey 🔹 🗔
	🔲 レガシ候補を使用する(U)
[診断(<u>D</u>) プロパティ	(P)) OK キャンセル

※なお、リモートネットワークをany以外に設定したい場合は、リモートネットワークのプルダウンメニュー右の"・・・" ボタンをクリックすることで下記の画面となりここで設定が可能です。

名前	IP アドレス	サブネット マスク
any	0.0.0	0.0.0
any6	0::0	0::0
		新規(<u>N)</u> 肖邶余(<u>R</u>)
Հット ワ− ታ ∕ዱ・	any	新規(<u>N)</u> 肖邶余(R)
、ットワーク名:	any	新規(N) 肖邶余(R)
ኣቃትワーク名: የ アドレス:	any 0.0.0.0	新規(<u>N)</u> 肖邶余(<u>R</u>)

下記のメッセージが表示された場合は、「はい」をクリックします。



セキュリティポリシータブの「10.10.1.1 (any)」を選択し、「プロパティ」をクリックします。



規則のプロパティ全般タブの一番上にある「設定」をクリックします。

リモート	エンドポイント	14	
	ゲートウェイ IP アドレス:	10.10.1.1	IP
J	リモート ネットワーク:	any	▼
IPsec /	IKE 候補		
	認証鍵	쿋 Si-R2_sharedkey	•]
9	候補テンプレート	normal	•
	IP アドレスを取得する 仮想 IP アドレスは、内部 です。	ネットワークのアドレス	設定)
□ 拡張	WZ証 VPN ゲートウェイでは、IKI または CHAP 認証が必要 す。	XAuth、RADIUS、 となる場合がありま	設定
		玄	至更(<u>C</u>)

IKE(フェーズ1)とIPsec(フェーズ2)の各パラメタを設定します。Si-R側の各設定と一致させる必要がありま す。「選択した値のみを候補に加える」にチェックをつけます。チェックを忘れた場合、正常にIPsecが張れない可能 性があるので必ずチェックを付けてください。

パラメータ候補	? ×
「YNN IKE 候補と IPsec	候補の各パラメータ値を設定します。
IKE 候補	
暗号化アルゴリズム:	AES-256 ~
整合性関数:	SHA256 \vee
IKE モード:	aggressive mode \sim
IKE グループ:	MODP 1536 (group 5) \sim
IPsec 候補	
暗号化アルゴリズム:	AES-256 ~
整合性関数:	HMAC-SHA256 \vee
IPsec モード:	tunnel \sim
PFS グループ:	MODP 1536 (group 5) \sim
☑ 選択した値のみを候補に力	加える
	 OK キャンセル

規則のプロパティ全般タブの中央にある、「仮想IPアドレスを取得する」にチェックをつけ、その右にある「設定」をクリックします。

リモート ネットワーク:	1	
	any	▼ [
E 候補		
21117年1月11日1月11日1月11日1日11日1日11日11日11日11日11日11日	📟 Si-R2_sharedkey	
戻補テンプレート:	normal	•
・アドレスを取得する	ן איירט-מעמצויט ר	說 走…
хжал ////////////////////////////////////		設定
証 /PN ゲートウェイでは、IKE たは CHAP 認証が必要 す。	:XAuth、RADIUS、 となる場合がありま	設定
	E 候補 Z証鍵: 実補テンプレート: P アドレスを取得する A DE IF アドレスは、Pha ^{DE} です。 証 IFN ゲートウェイでは、IKE たたは CHAP 認証が必要 す。	E 候補 認証鍵:

仮想IPアドレスの設定を行います。仮想IPアドレスとはプライベートネットワークへアクセスする際ここの端末が仮想的に利用するIPアドレスとなります。

「手動で指定」を選択し、IPアドレスとサブネットマスクを設定してください。ここで設定した、"20.1.1.1"はSi-R 側のtemplate 0 ip route 0と一致している必要があります。

仮想 IP アドレス	8 3
しています。 使想 IP アド 行います。	レスに割り当てるプロトコルを選択するか、手動で設定を
プロトコル 〇 IPsec 経由の DHe 〇 L2TP (Layer Tw 〇 IKE 設定モード	CP (Dynamic Host Configuration Protocol) o Tunneling Protocol)
 ● 手動で指定: 	
IP アドレス:	20.1.1.1
サブネット マスク:	255.255.255.0
DNS サーバと WI	NS サーバを指定する:
DNS サーバ:	
WINS サーバ	
	OK キャンセル

規則のプロパティ詳細タブの「NAT装置を経由する」にチェックをつけます。NAT Traversalを選択します。

271	リティの関連付けの有効期間 IPsec セキュリティと IFL セキュリティの関連付 Exact はまましょう
Ears-1	「切り有効期間を設定します。
	✓ この規則を監査する(A)
詳細才	วังรุ่ม
學	□ IP 圧縮を適用する① ■ DMTU (Path Maximum Transfer Unit) を発見する(M) ■ NAT 装置を経由する ● NAT Traversal ■ YAMAHA ■ 常に使用する
	◎ UDP カブセル化 ポート: 2746
	EDPD(Dead Peer Detection)を使用する(D) 問題(秒): 再試行(同):
-NA	 記載時(ご覧)(S) ① 切断時(ご再接続する(R) ⑦ 分割トンネリングを拒否する T-T & IP 圧縮結報 NAT-T と IP 圧縮を同時(ご選択することはできません (前者は後 まちせポートしません).

設定が終了したら、規則のプロパティで「OK」をクリックします。

印え 目	╪結曲 エ`ンドポイ`ント		
	ゲートウェイ IP アドレス:	10.10.1.1	IP
T.	リモート ネットワーク:	any	-
IPsec /	IKE 候補	N:	
??	認証鍵	🐖 Si-R2_sharedkey	•
U	候補テンプレート	normal	•
	* IF アドレスを取得する 仮想 IP アドレスは、内部 です。 WPN ゲートウェイでは、IKE または CHAP 認証が必要 す。	ネットワークのアドレス E XAuth、RADIUS、 そとなる場合がありま	設定 設定
		変更	<u>[(C)</u>

「適用」をクリックします。設定は完了です。

	デフォル	· k	 •]	
	Psec 前フィル? VPN 接続	8		1000
	避 10.10.1.1 (a 通 追加…	any)		現目
	セキュアな接続	<u>п_</u> л		0
	デフォルト応答			評
	iPsec 後フィル! すべてのトラフィ	タ ックを許可		備
				RR A
				10
Carro				The second
		岩(昭令/ 内)	-/n) [=0#6(D)
19/1	<u>кө</u> ,	HUNDA(E)		а́≲⊎л(<u>D</u>)
説明				

Dit_NET-G診断方法

診断を行うことで、NET-G、およびSi-R側の設定が正しいかを確認可能です。 セキュリティポリシータブで先ほど作成した10.10.1.1 (any)を選択し、診断をクリックします。

#リシー: Ⅲ- ● ■	i デフォ Psec 前フィル	μト ιφ	AN	•	
	VPN 接続 費 10.10.1.1 ひきュアな接続 セキュアなネッ デフォルト応答 Psec 後フィノ すべてのトラフ	(any) 売 トワーク F レタ イックを許可			規則の評価順序
追加	(<u>A</u>) (削除(<u>B</u>)) (לחלד (ם)		<u>کالہ (D)</u>

設定に問題が無ければ以下の結果が表示され、IKE SAとIPsec SAが正常に確立されていることが確認できます。

ŕ			>
診断がデ す。接続	E了しました。リモート(側との リペラメータを表示するには、	IPsec で保護さ [詳細] ボタンをク	れた接続を確立できま リックしてください。
		<< 言羊紙	l(<u>D</u>) 終了
調査結果			
	接続のプロパ	<u>7</u> ≁	
リモート:	10.10.1.1		
ペンター ID:	E 11 JAN		
仮想 IP:	20.1.1.1		
	IKE	SA	
21:	既知共有鍵	÷−F	aggressive
暗号化:	aes-cbc (256 ビット)	グループ:	MODP 1536
ハッシュ:	sha256	有効期間:	0MB/14400s
NAT-T:	有効		
	IPsec	SA	
ブロトコル:	ESP	モード	トランスポート
暗号化:	aes (256 분ット)	PFS グループ	7: MODP 1536
HMAC:	hmac-sha256-128	有効期間:	400MB/3600s
IPComp:	なし		